

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

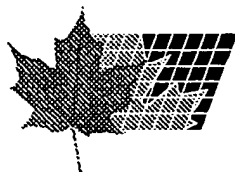
Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



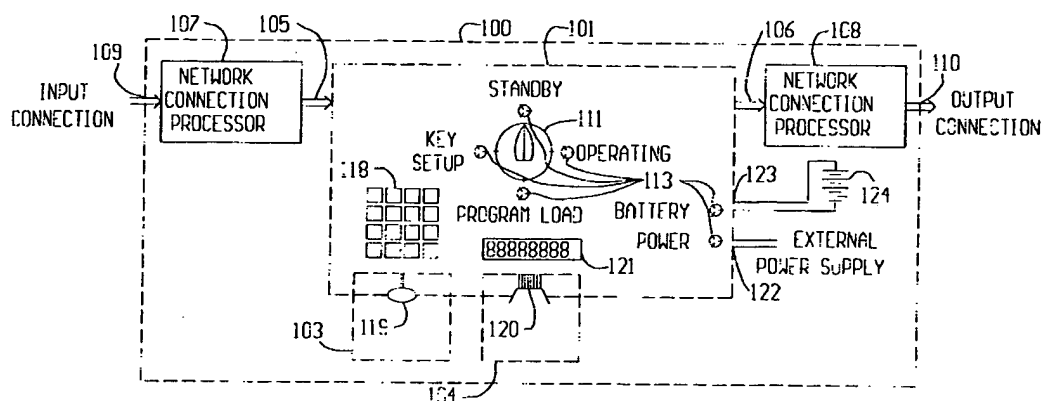
(72) MOREAU, Thierry, CA

(71) CONNOTECH EXPERTS-CONSEILS INC., CA

(51) Int. Cl.⁶ H04L 9/30

(54) **APPAREIL CRYPTOGRAPHIQUE A CLE REVELEE COTE-SERVEUR AVEC CLES SECRETES DE PROTECTION ET D'ISOLEMENT DE RESEAUX PUBLICS**

(54) **SERVER-SIDE PUBLIC KEY CRYPTOGRAPHY APPARATUS WITH PRIVATE KEY PROTECTION AND ISOLATION FROM PUBLIC NETWORKS**



(57) A server-server public-key cryptography apparatus is disclosed for use in the computer facilities of central organizations, e.g. on-line service providers. The apparatus has two network connections of the type common to computer networks, used respectively for exclusively receiving input data and exclusively transmitting output data for some elementary private key computation (digital signature, public key decryption, secret key establishment primitive based on a public key algorithm). The secrecy of this private key is supported by a number of the present invention features. Among others, are provided the cryptographic key management operations needed to initially configure, operate, maintain, and re-install in the case of disaster recovery. In operations, the access to the elementary private key computation has to be restricted to those computer applications that are the legitimate users of the private key. The one-way input connection, the one-way output connection, and some features of the cryptographic key management operations are provided to secure this restricted access to the function performed by the secure computing device.

ABSTRACT

A server-server public-key cryptography apparatus is disclosed for use in the computer facilities of central organizations, e.g. on-line service providers. The apparatus has two network connections of the type common to computer networks, used respectively for exclusively receiving input data and exclusively transmitting output data for some elementary private key computation (digital signature, public key decryption, secret key establishment primitive based on a public key algorithm). The secrecy of this private key is supported by a number of the present invention features. Among others, are provided the cryptographic key management operations needed to initially configure, operate, maintain, and re-install in the case of disaster recovery. In operations, the access to the elementary private key computation has to be restricted to those computer applications that are the legitimate users of the private key. The one-way input connection, the one-way output connection, and some features of the cryptographic key management operations are provided to secure this restricted access to the function performed by the secure computing device.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

- 1 A secure cryptographic device implementing a public key cryptography primitive with a one-way input connection and a one-way output connection.
-

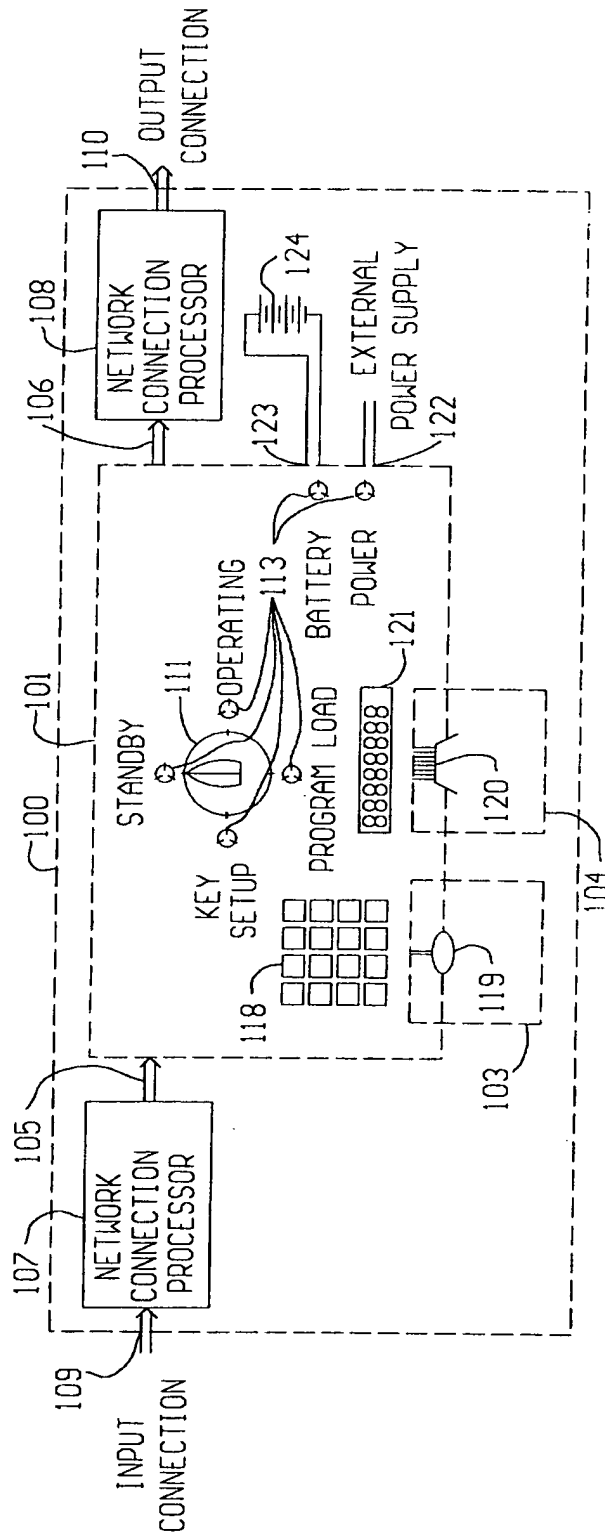


Figure 1

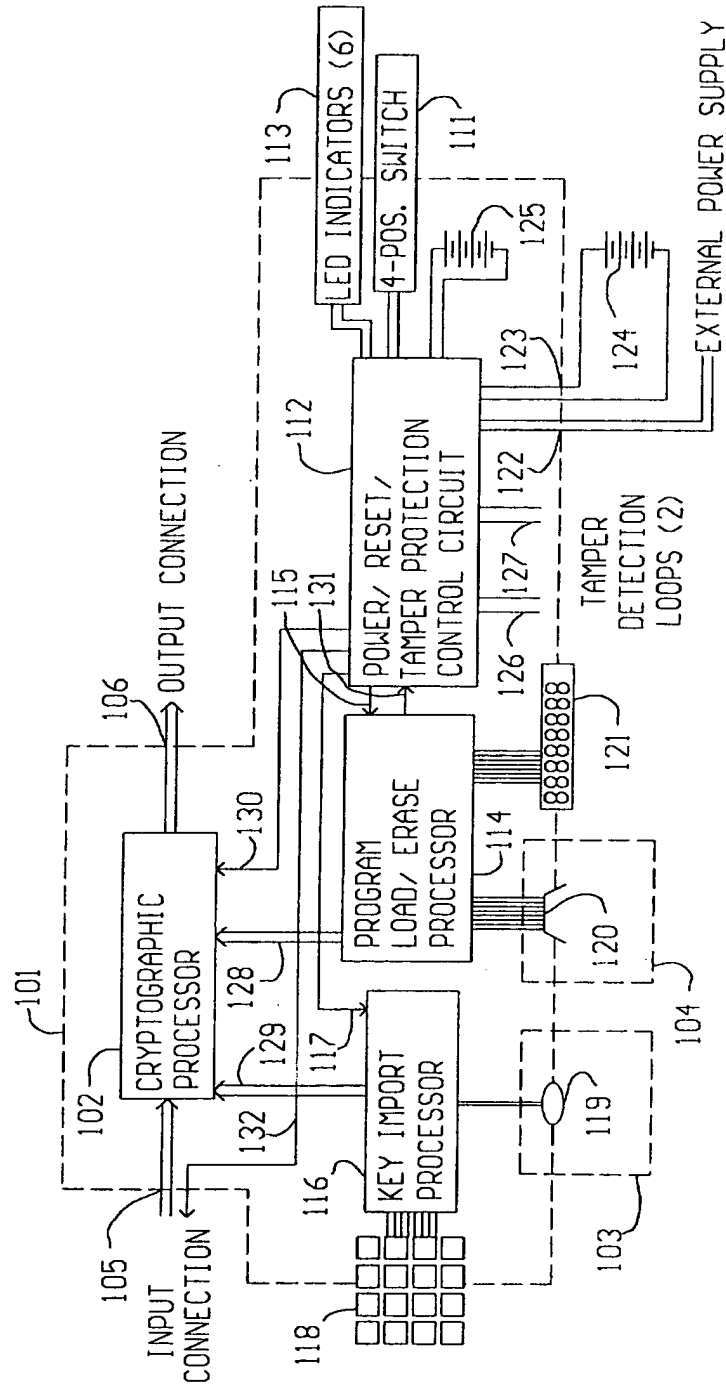


Figure 2

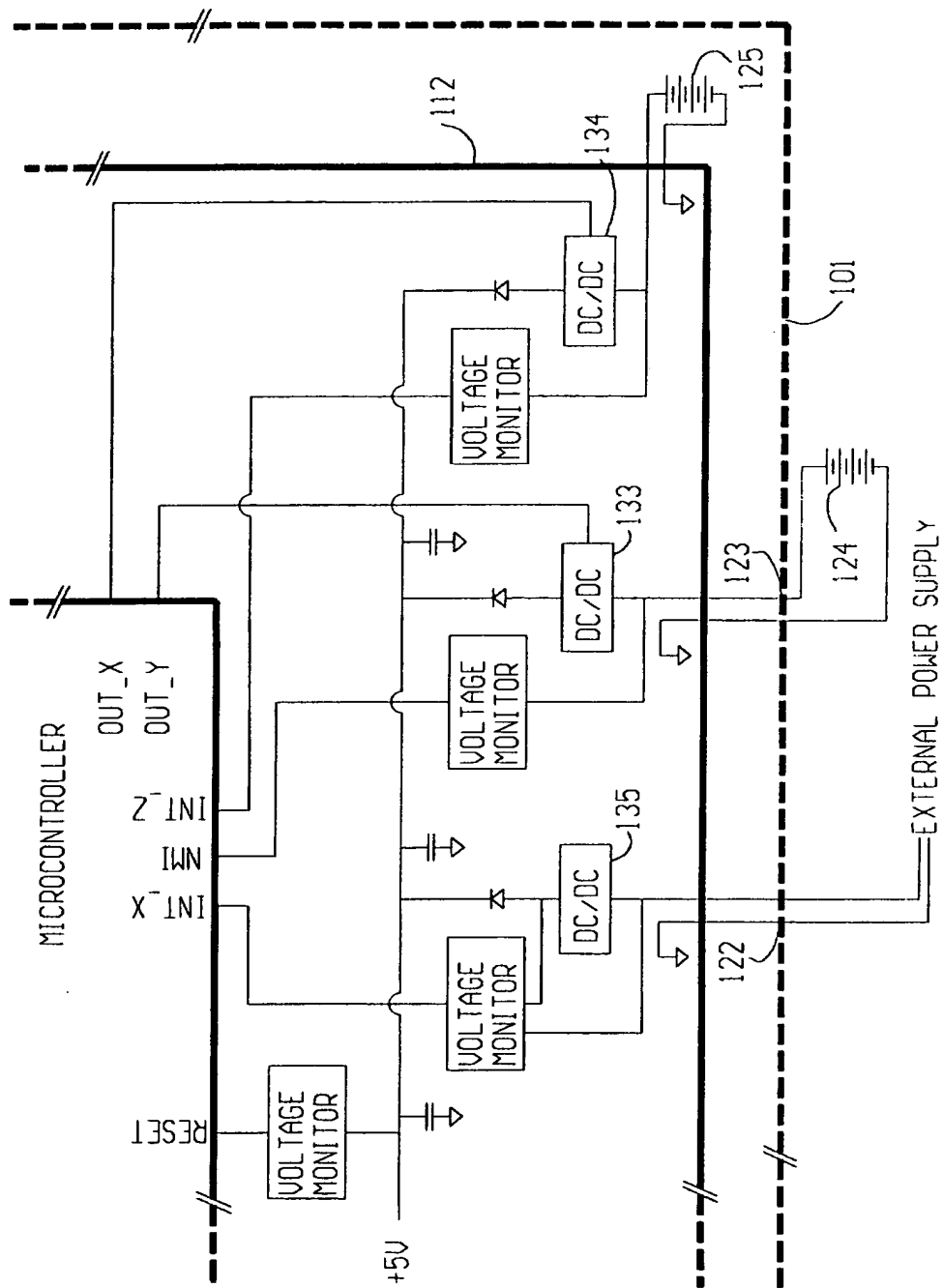


Figure 3

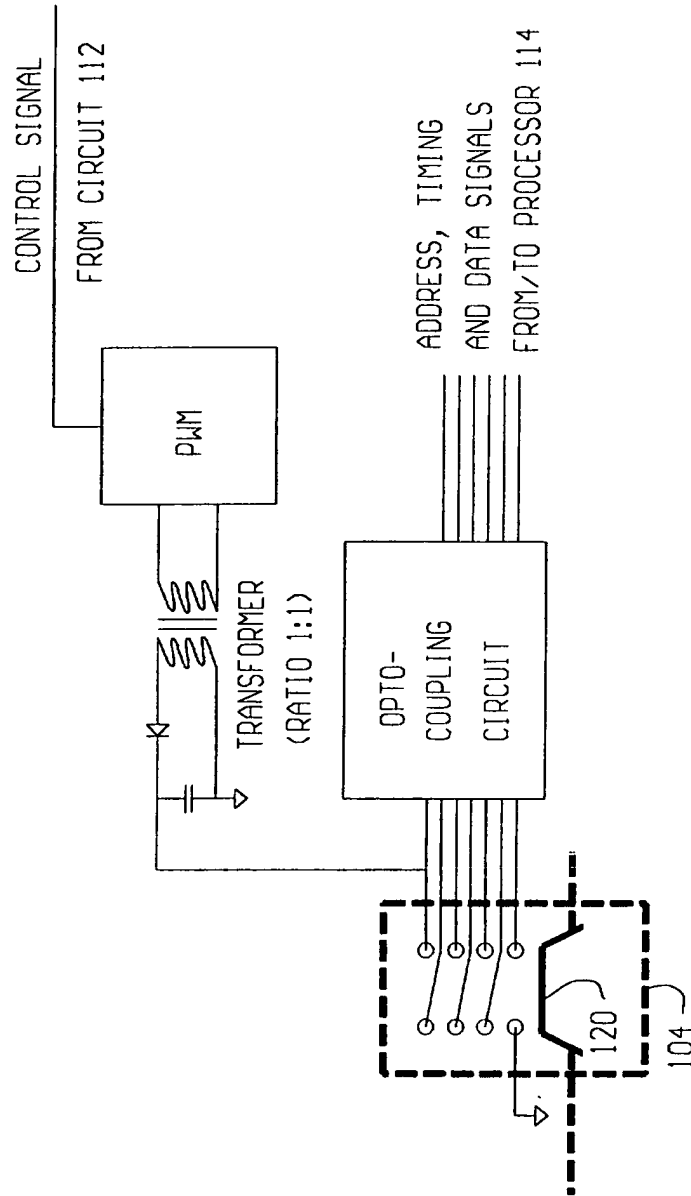


Figure 4

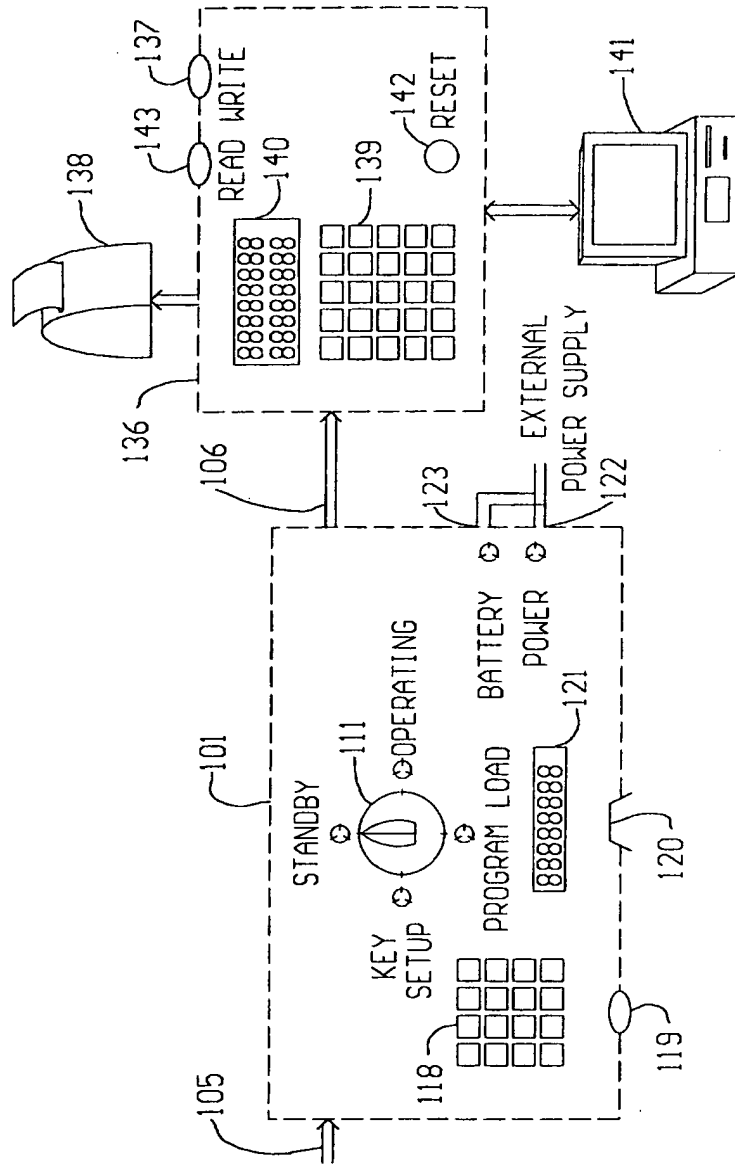


Figure 5